View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Elsevier - Publisher Connector

Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 93 (2016) 760 – 767

Procedia Computer Science

6th International Conference On Advances In Computing & Communications, ICACC 2016, 6-8 September 2016, Cochin, India

An Optimal (k,n)Visual Secret Sharing Scheme for Information Security

Mahmoud E. Hodeish[a], Linas Bukauskas[b],Vikas T. Humbe[c]*

[a] *School of Computational Sciences, Swami Ramanand Teerth Marathwada University, Nanded-431606, M.S., India*
[b] *Faculty of Mathematics and Informatics, Vilnius University, Didlaukio 47, Vilnius Lithuania*
[c] *School of Technology, Swami Ramanand Teerth Marathwada University, Sub-center Latur-413512, M.S., India*

Abstract

Recently, based on the concept of Visual Secret Sharing (VSS) scheme proposed by Naor and Shamir in 1994, many of schemes have been proposed to protect the security of binary image. Yet, the problems of pixel expansion, extensive codebook designs, and lossy recovery are still unsolved. The current paper attempts to propose a new (k,n) scheme to refute the pixel expansion based on codebook and transpose of matrices. This scheme will offer promising solutions for the security condition, computation complexity, storage requirement, fast network transmission, and reconstructing the secret image accurately without any distortion.

© 2016 The Authors. Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

Peer-review under responsibility of the Organizing Committee of ICACC 2016

Keywords: Visual Secret Sharing; Visual Cryptography; Pixel Expansion; PSNR; Visual Information.

1. Introduction

Visual information is a type of data that is used for authentication purposes such as biometric devices, medical diagnosis, and e-court evidence. However, with the current rapid advancement in networking and the large number of communication channels such as Internet, Wi-Fi, and other techniques, the access into visual information has become easy. Therefore, it becomes a necessity to secure visual information during transmission through public network from the unauthorized users. To resolve the problem of information security, a lot of scholars have proposed different techniques and methods such as Visual Cryptography (VC) as a new encryption technique used to secure and hide visual information.

* Corresponding author. Tel.: 0091-989-074-3372.
E-mail address: mah_hodeish@yahoo.com

1877-0509 © 2016 The Authors. Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).
Peer-review under responsibility of the Organizing Committee of ICACC 2016
doi:10.1016/j.procs.2016.07.288

The VC has been proposed by Naor and Shamir [1]. It is also called a Visual Secret Sharing (VSS) that is used to encrypt the secret message in visual form by splitting it into *n* shares that can, then be transmitted securely via internet or any other communication channels. As the secret message can only be decrypted when a sufficient number of shares superimposing together [2].

The important feature of the VSS scheme is that the decryption side can easily be done by Human Visual System (HVS) without using a complex computation that requires more time for decryption. In addition, there are other features that have attracted people's attention such as imperceptibility, security, high capacity, and reversibility [3].

As a basis for the VC method, a secret sharing was firstly introduced by Shamir [4] and Blakly [5] as the simplest method to secure information. Usually, this scheme can be implemented as (k,n) scheme with *n* participants and with *k* threshold, in such that $k \leqslant n$ [6]. The basic idea of (k,n) method is sharing a secret message *s* among *n* participants; one share for each of them. In this regard, the following conditions should be held:

- No participant knows the share given to another participant.
- *k* together can reveal the secret image by superimposing *k* (transparencies).
- Any *t* transparencies, $t < k$, the secret cannot be decoded.

It is worth noting that the secret sharing scheme is supposed to be a bank vault that must be passed by a secret key, and to provide a good solution in many real-life applications [7-8].

The VSS scheme is the second method. It was, firstly, invented and innovated by Naor and Shamir in 1994 for protecting the security of visual information transmitted to different participants over public network. According to them, this method is expressed as *k*-out-of-*n* secret sharing. The concept of this scheme is illustrated as follows; the secret image is divided into *n* shares so that the original image is visible if any *k* of these shares are stacked together. The image remains hidden if fewer than *k* shares are superimposed together. The construction of shares can be done by using a codebook to encode a binary image with different pixel expansion as following:

A. Two-out-of-two scheme (2 subpixels):

In this scheme, a secret binary image is encoded by using a codebook (shown as table 1) into two shares as shown in fig. 1 (a). Each pixel *(p)* in the secret image is split into two subpixels (black/white and white/black) located next to each other in each of the two generated shares. If a *p* is white, four pixels will be selected randomly from the pixels opposite to the white pixel in the codebook. In contrast, if a *p* is black, four pixels will be selected randomly from the pixels opposite to the black pixel in the codebook. Finally, two shared images, as shown in fig. 1 (c) and (d), will be constructed and transmitted to different participants. When these shares are superimposed, the original information can easily be reconstructed by the human eyes as shown in fig. 1

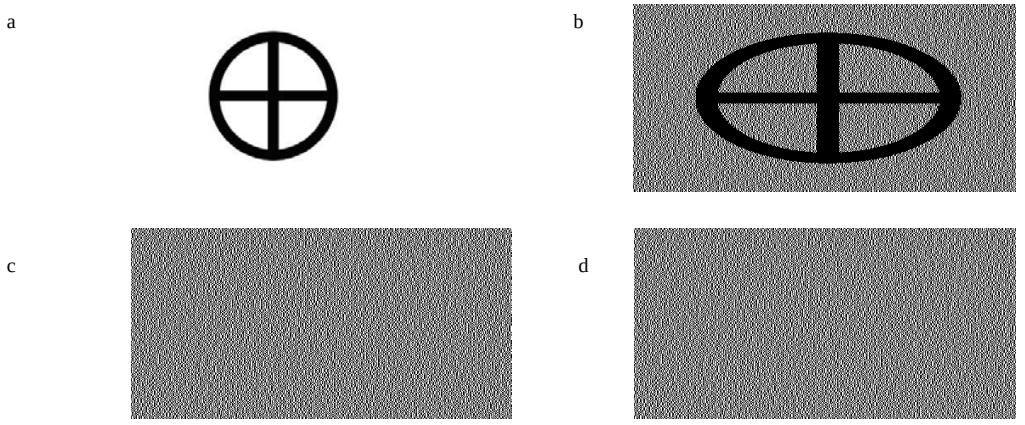


Fig. 1. Two out of two (2 subpixels) scheme, (a) the secret image, (b) and (c) the shared images and (d) the reconstructed image.

B. Two-out-of-two scheme (4 subpixels):

In practice, the (2,2)- VC scheme with 2 subpixels expansion can change the aspect ratio of the original image and leads to the loss of some information, and for this reason, Naor and Shamir suggested to use four subpixels expansion by using a codebook. Here, the secret image is encoded into two shared images. In case if a pixel is white, two blocks will be chosen randomly from the left side of the codebook. In contrast, if a pixel is black, two blocks will be chosen randomly from the right of the codebook, then two shared images will be constructed. Finally, the original information can be obtained by superimposing the two shared images together.

Table 1. The codebook of (2,2) secret sharing scheme (two pixel expansion).

Pixel	Share1	Share2	Probability
			1/2
			1/2
			1/2
			1/2

To avoid the use of the pixel expansion, Ito et al. [9] proposed a new scheme with using the traditional (k,n) scheme with no pixel expansion. In addition to the use of the traditional VSS, this scheme uses a Boolean n-Vector $V= [v_i \ldots\ldots v_n]^T$, where v_i represents the pixel in *i-th* shared images. To obtain the original image, traditional OR-ing operation is used to all pixels in *V*. Moreover, a probabilistic scheme also proposed by Yang [10] to deal with size invariant shares in which the frequency of white pixels is used to show the contrast of the reconstructed image. This scheme is non-expansible and based on the conventional VSS scheme. The non-expansible term means that the size of shared images and original image is the same.

Recently, many schemes have been proposed to solve the problem of invariant shares sizes and invariant aspect ratio [11, 12, and 13]. Non-expansible scheme proposed by Hodeish & Humbe [14], which is easily to be implemented by taking two neighbouring pixels in turn to generate the shared images with the same size of the original image. This scheme provides a quite enough quality for the regenerated image, but the distortion is still there.

The methods discussed earlier can provide solutions for the security of binary image. Yet, the problems of pixel expansion, extensive codebook designs and contrast of reconstructed image are still unsolved. In this paper, a new (k,n) scheme based on codebook, transport of matrices, Boolean n-Vector, and XORing operation is proposed. Under this method, codebook has been designed to refute the pixel expansion. Then based on the codebook, Boolean *n-vector* is used to generate the shared images. Thus, only the authorized person can obtain the original image without distortion.

The remaining part of this paper is organized as follows: Section 2 describes the proposed method in details. Experimental results and performance analysis are provided in section 3. Finally, the conclusion is drawn in section 4.

2. The Proposed Scheme

Here, the proposed scheme uses the codebook which is designed on a set of matrices of the traditional VC presented as follows:

C_0= { *all the matrices obtained by permuting the columns of* $\begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \ldots & 0 \\ \cdots & & \cdots & & \cdots \\ 1 & 0 & 0 & \cdots & 0 \end{bmatrix}$ }

C_1= { *all the matrices obtained by permuting the columns of* $\begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \ldots & 0 \\ \cdots & & \cdots & & \cdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}$ }

Here, matrix C_0 denotes the matrix for constructing shares for the white pixels and C_1 for the black ones. Depending on C_0 and C_1 matrices, we have designed the codebook for the proposed scheme. The basic matrices used in the proposed scheme are as follows:

$$C_0 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}, \qquad C_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

In this scheme, the transpose of above matrices is used, then permute all columns to get the codebook used here.

$$C_0^T = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \qquad C_1^T = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

2.1 Algorithm

Step 1. Take one pixel as one time input *P* from the secret image.

Step 2. For *P*, determine whether it is

a. Black b. White

Step 3. If the color of *P* is

1. Black,

a. Randomly select one block from the four blocks that is peer to the black pixel in the codebook (shown as a table 2).

b. Randomly select one row from the selected block and assign it to vector *V*.

2. White,

a. Randomly select one block from the four blocks that is peer to the white pixel in the codebook (shown as a table 2).

b. Randomly select one row from selected block and assign it to vector *V*.

Step 4. *V= [v1, v2, v3, v4]*, constructs four shares as:

share1= v1, share2= v2, share3= v3, share4= v4.

Step 5. Repeat the steps from 1 to 5 until all pixels of the secret image are shared.

Step 6. To reconstruct the original image, use XOR-ing operation in order to superimpose any order of shares for different construction as follows:

(2,4): share1⊕share2 or share1⊕share3 or share1⊕share4 or share2⊕share3 or share2⊕share4 or share3⊕share4.

(3,4): share1⊕share2⊕share3 or share1⊕share2⊕share4 or share1⊕share3⊕share4 or share2⊕share3⊕share4.

(4,4): share1⊕share2⊕share3⊕share4.

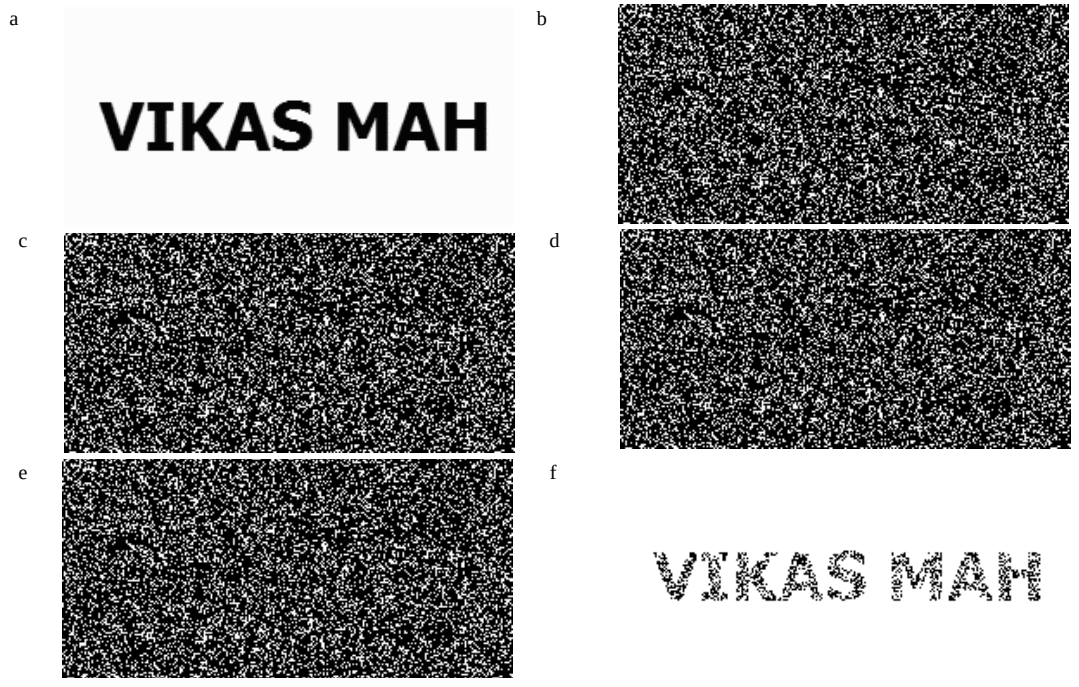
Where ⊕ indicates the XOR operation.

Table 2. The codebook of the proposed scheme.

Pixel	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4
■	■					■					■					■
		■					■					■	■			
			■					■	■					■		
				■	■					■					■	
□	■	■	■	■												
					■	■	■	■								
									■	■	■	■				
													■	■	■	■

3. Experimental Results and Performance Analysis

The binary text image with size of 261×127 is taken as a secret image as shown in fig. 2 (a) to conduct the experiment of the proposed scheme. The codebook is designed based on the transport of basic matrices that are used in the current scheme. Firstly, one pixel is taken as input by raster-scan order. Then each pixel of secret image is successively taken into the codebook of this scheme in order to generate four shares with the same size of the original secret image as shown in fig. 2 (b), (c), (d) and (e). As you can notice, fig. 2 (h) shows the recovered image by superimposing the four shared images by performing XORing operation without distortion.



g h

Fig. 2. The proposed scheme, (a) the secret image, (b),(c),(d), and (e) the shared images , (f) the reconstructed image(share1&2), (g) the reconstructed image(share1,2&3), (h) the reconstructed image(share1,2,3&4).

The XORing operation permits the complete restoration of secret image [15]. The XOR-based VC was firstly suggested to increase the quality of the reconstructed image and solve the problem of pixel expansion [16]. The reconstructed image by superimposing two or three shared images together also has a quite good contrast as shown in fig. 2 (f) and (g).

3.1 Performance Analysis

The proposed scheme results in the following advantages: (1) The reconstructed images have the same size of the original secret image that means that the pixel expansion equals one. (2) Due to that it saves the storage space of the participants, provides fast transmission via public network, Internet, and other communication channels. (3) The image obtained after stacking the shared images appears accurately. In addition, in case of reconstructing (4,4) for the proposed scheme by using XOR operation, the reconstructed image quality increases and there is no distortion. This can be evaluated by Peak Signal-to-Noise Ratio (PSNR) which is used to measure the visual quality of the recovered image with respect to the original image.

To calculate the PSNR, the Mean Squared Error (MSE) should be calculated first. The PSNR and MSE can mathematically be expressed as eq. (1) and eq. (2):

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (h_{ij} - h'_{ij})^2 \quad (1)$$

$$PSNR = 10 \times \log \frac{R^2}{MSE} \quad (2)$$

Fundamentally, while the MSE value should be as low as possible, the PSNR should be higher. A higher PSNR indicates lower variation between the secret image and the reconstructed image with a good visual quality. However, when the PSNR value is equal to ∞, it indicates that the scheme provides a maximum visual quality [17-18].

Table 3 shows the obtained values of MSE and PSNR between the original image and the recovered image of each possible construction of the proposed scheme.

Table 3. The MSE and PSNR values of the possible constructions of the proposed scheme.

The proposed scheme	MSE	PSNR
(2,4)	0.0482	13.1687
(3,4)	0.2512	5.999
(4,4)	0	∞

For the proposed scheme in case of (4,4), the obtained values of PSNR and MSE are ∞ and 0, respectively. These values prove that the proposed method, especially in case of (4,4), is optimal due to the fact that there is no any difference between the recovered image and the original secret image.

Recently, many of visual secret sharing schemes have been proposed for securing the secret image. The current results in comparison with the some previously published schemes are shown in the table 4.

Table 4. The results in comparison to some published schemes.

Scheme	Secret image	Pixel expansion	Aspect ratio	Reconstructed image	
Ito et al.'s scheme 1999	Binary (m×n)	1	Unchanged		Lossy
Yang's scheme 2004	Binary (m×n)	1	Unchanged		Lossy
Yang and Chen's scheme 2005	Binary (m×n)	Variable	Changed		Lossy
Yang and Chen's scheme 2006	Binary (m×n)	Variable	Changed		Lossy
Pal et al.'s scheme 2010	Binary (m×n)	Variable	Changed		Lossy
Proposed scheme	Binary (m×n)	1	Unchanged	(2,4)	Quite good
				(3,4)	Lossy
				(4,4)	Lossless

4. Conclusion

In recent years, methods of secret sharing have been developed for VC based on the Naor and Shamir method. Yet, the pixel expansion and distortion of recovered secret image are still the main challenges and problems that have been unsolved. In the present paper, a new method has been proposed to solve such issues. The proposed method is to refute the pixel expansion based on codebook and transport of matrices in order to get hold the security of secret image and solve the problem of pixel expansion and the lossy of recovered image. From the experimental results, the shared images in the proposed scheme have the same size of the original secret image. Moreover, by using XORing operation, the secret image can perfectly be recovered, especially in case of XORing four shared images together. Furthermore, the proposed method provides fast transmission via public network, Internet, and other communication channels.

Future work can develop an image sharing method for gray-level images with enhancing the security of shares against of number of attackers they have an ability to collect all the shares passing in sequence over the network.

Acknowledgements

The authors would like to express their deepest thank and gratitude to Dr. G. V. Chowdhary, Ph.D. (IIT, Madras), Director of School of Computational Science for his ceaseless valuable suggestions and constant encouragement. Also the authors would like to express their thanks to Hodeidah University and S.R.T.M University for their unlimited supports and encouragement.

References

1. M. Naor, and A. Shamir. Visual Cryptography. In: Advances in Cryptography-Eurocrypt '94, vis Lecture Notes in Computer Science 950; 1994. p. 1–12.
2. Himanshu Sharma, Neeraj Kumar and Govind K. Jha. Enhancement of security in Visual Cryptography system using Cover Image share embedded security algorithm (CISEA). In: International Conference on Computer & Communication Technology (ICCCT); 2011. p. 462–467.
3. Wei-Kuei Chen. Image Sharing Method for Gray-level Images. In: The Journal of Systems and Software 86; 2013. p. 581-585.
4. A. Shamir. How to share a secret. In: Communications of the ACM 22; 1979. p. 612-613.
5. G.R. Blakley. Safeguarding cryptographic keys. In: Proceedings of the National Computer Conference, American Federation of information Processing Societies Proceedings 48; 1979. p. 313-317.
6. C.-N. Yang, C.-Y. Lin. Almost-aspect-ratio-invariant visual cryptography without adding extra subpixels. In: Inform. Sci.; 2015. p. 1-20.

7. Wu,C.-C., Kao, S.-J., Hwang, M.-S. A high quality image sharing with steganography and adaptive authentication scheme. In: The Journal of Systems and Software 84; 2012. p. 2196-2207.
8. Hodeish, M.E.; Humbe V.T. State-of-the-Art Visual Cryptography Schemes. In: International Journal of Electronics Communication and Computer Engineering, vol. 5; 2014. p. 412-420.
9. Ryo Ito, Hidenoir Kuwakado, and Hatsukazu Tanaka. Image size invariant visual cryptography. In: IEICE Transaction, E82-A; 1999. p. 2172-2177.
10. Ching-Nung Yang. New visual secret sharing schemes using probabilistic method. In: Patteren Recognition Letters 25(4); 2004. p. 481-494.
11. Ching-Nung Yang and Tse-Shih Chen. Aspect ratio invariant visual secret sharing schemes with minimum pixel expansion. In: Patteren Recognition Letters 26(2); 2005. p. 193-206.
12. Ching-Nung Yang and Tse-Shih Chen. New size-reduced visual secret sharing schemes with half reduction of shadow size. In: IEICE Transaction, 89-A (2); 2006. p. 620-625.
13. Jayanta Kumar Pal, J. K. Mandal and Kousik Dasgupta. A (2, N) visual cryptographic technique for banking applications. In: International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.4; 2010. p. 118-127.
14. Hodeish, M.E.; Humbe, V.T. A (2,2) secret sharing scheme for visual cryptography without Pixel Expansion. In: Electrical, Electronics, Signals, Communication and Optimization (EESCO), 2015 IEEE International Conference on , vol., no.; 2015. p.1-7.
15. Pim Tuyls, Henk D. L. Hollmann, Jack H. Van Lint, and Luds M. G. M. Tolhuizen. XOR-based Visual Cryptography Schemes.in: Designs, Codes and Cryptography 37(1); 2005. p. 169–186.
16. D. Ou a, W. Sun and X. Wu. Non-expansible XOR-based visual cryptography scheme with meaningful shares. In: Signal Processing 108; 2015. p. 604–621.
17. Angel Rose A and Sabu M Thampi. A Secure Verifiable Scheme for Secret Image Sharing. In: Procedia Computer Science 58; 2015. p. 140 – 150.
18. Shankar K and Eswaran. Sharing a Secret Image with Encapsulated Shares in Visual Cryptography. In: Procedia Computer Science 70; 2015. p. 462 – 468.